

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-007288

(43)Date of publication of application : 11.01.2002

(51)Int.Cl.

G06F 13/00

G06F 12/14

G06F 15/00

G09C 1/00

H04L 9/32

(21)Application number : 2000-186279

(71)Applicant : NTT COMMUNICATIONS KK

(22)Date of filing : 21.06.2000

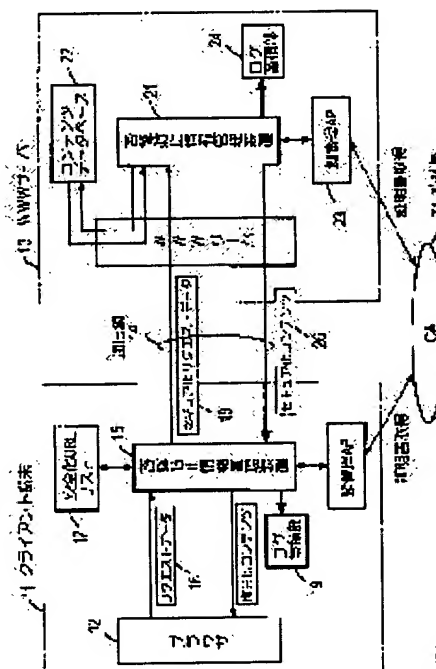
(72)Inventor : YASUDA HITOSHI
WATANABE TORU
OGIWARA TOSHIHIKO
TABUCHI HIROYASU

(54) METHOD AND DEVICE FOR MANAGING NEGATION PREVENTION INFORMATION, AND PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To store a log of transmitted or received information in a safe state such that it cannot be negated later.

SOLUTION: A browser 12 sends out a GET Request 16, and then when acquisition in a secured state is desired, a managing device 18 detects of this by a secure URL list 17, adds key information on a client in it to the Request 16, and sends them to a server 12. The server 12 extracts contents corresponding to the Request, and the managing device 21 gives a signature thereto, ciphers the contents with the open key of the client based upon the key information, and stores the ciphered contents in a log 24 and also sends them in client MOSS format, while indicating that the data are ciphered data in its header. The managing device 15 stores the ciphered contents in a log 19 and then deciphers the contents.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

【特許請求の範囲】

【請求項 1】 アプリケーションデータに対し、送信者の電子署名を行い、その署名付アプリケーションデータをログ蓄積部に蓄積すると共に相手方へ送信することを特徴とする否認防止情報管理方法。

【請求項 2】 上記署名付アプリケーションデータをログ蓄積部に蓄積するに先立ち、暗号化して上記蓄積を行うと共に相手方へ送信することを特徴とする請求項 1 記載の否認防止情報管理方法。

【請求項 3】 受信した署名付アプリケーションデータをログ蓄積部に蓄積し、上記受信した署名付アプリケーションデータに対し、その署名の検証を行い、その検証に合格すると、上記署名付アプリケーションデータを真として処理することを特徴とする請求項 1 記載の否認防止情報管理方法。

【請求項 4】 上記受信した署名付アプリケーションデータは暗号化されたものであり、その暗号化された署名付アプリケーションデータを上記ログ蓄積部に蓄積し、上記暗号化された署名付アプリケーションデータを復号し、その復号した署名付アプリケーションデータに対して上記署名検証を行うことを特徴とする請求項 1 又は 2 記載の否認防止情報管理方法。

【請求項 5】 上記送信アプリケーションデータはブラウザから出力されたものであり、それが GET か POST か判定し、POST であれば上記暗号化の鍵を、サーバからブラウザに送られた鍵情報にもとづき取得し、上記ブラウザからの出力が GET であれば、上記アプリケーションデータに対し署名、暗号化をすることなく、送信者の鍵情報を追加して送信することを特徴とする請求項 1 乃至 4 の何れかに記載の否認防止情報管理方法。

【請求項 6】 先ず安全化条件を満たすかを判断し、安全化条件を満たすと、上記電子署名とそれ以後の処理を行い、安全化条件を満たさないと、上記アプリケーションデータを上記ログ蓄積部に蓄積することなく、そのまま送信することを特徴とする請求項 1 乃至 5 の何れかに記載の否認防止情報管理方法。

【請求項 7】 クライアント端末からの鍵情報はアプリケーションデータを受信し、その受信したアプリケーションデータに付加された鍵情報を一時保存し、上記受信したアプリケーションに応じたコンテンツを含むアプリケーションに対し、電子署名を行い、その署名付アプリケーションを上記保存した鍵情報にもとづき暗号化し、その暗号化アプリケーションデータをログ蓄積部に蓄積すると共に上記クライアント端末へ送信することを特徴とする否認防止情報管理方法。

【請求項 8】 クライアント端末からの鍵情報付アプリケーションデータを受信し、その受信したアプリケーションデータに付加された鍵情報を一時保存し、

上記受信したアプリケーションに応じた、署名付コンテンツを含むアプリケーションを上記保存した鍵情報にもとづき暗号化し、

その暗号化アプリケーションデータをログ蓄積部に蓄積すると共に上記クライアント端末へ送信することを特徴とする否認防止情報管理方法。

【請求項 9】 クライアント端末からの鍵情報付暗号化されたアプリケーションデータを受信し、その暗号化されたアプリケーションデータをログ蓄積部に蓄積し、かつ上記アプリケーションデータに付加された鍵情報を一時保存し、

上記暗号化されたアプリケーションデータを復号し、その復号されたアプリケーションデータの署名を検証し、

その検証に合格すると、上記アプリケーションデータにもとづき、上記クライアント端末へ送信するアプリケーションデータが安全化の条件を満たすか否かを判断し、その条件を満たさなければ、そのままそのアプリケーションデータを送信し、条件を満たせば、そのアプリケーションデータに対し電子署名を行い、その署名付アプリケーションデータを上記一時保存した鍵情報にもとづき暗号化し、その暗号化されたアプリケーションデータをログ蓄積部に蓄積すると共に送信することを特徴とする否認防止情報管理方法。

【請求項 10】 受信した署名付アプリケーションデータをログ蓄積部に蓄積し、上記署名付アプリケーションデータに対し、その署名の検証を行い、その検証に合格すると、上記署名付アプリケーションデータを真として処理することを特徴とする否認防止情報管理方法。

【請求項 11】 上記受信した署名付アプリケーションデータは暗号化された署名付アプリケーションデータであり、

上記ログ蓄積部への蓄積は上記暗号化された署名付アプリケーションデータに対し行い、上記暗号化された署名付アプリケーションデータに対し復号を行い、その復号された署名付アプリケーションデータに対し、上記署名の検証を行うことを特徴とする請求項 10 記載の否認防止情報管理方法。

【請求項 12】 請求項 1 乃至 11 の何れかの方法をコンピュータに実行させるプログラムを記録した記録媒体。

【請求項 13】 アプリケーションプログラムにより動作するアプリケーション手段と、通信路との間に設けら

れる否認防止情報管理装置であって、
 通信路より受信した暗号化アプリケーションデータが蓄積されるログ蓄積部と、
 上記暗号化アプリケーションデータを復号する復号部と、
 上記復号されたアプリケーションデータの署名を検証する検証部と、
 上記検証部の検証に合格したアプリケーションデータを上記アプリケーション手段へ送る手段と、
 を具備する否認防止情報管理装置。

【請求項 14】 アプリケーション手段から受け取ったアプリケーションデータに対し電子署名を行う署名部と、
 上記署名付アプリケーションデータを送信先の鍵情報にもとづき暗号化する暗号部と、
 上記暗号化されたアプリケーションデータが蓄積されるログ蓄積部と、
 上記蓄積された暗号化されたアプリケーションデータを通信路へ送信する手段と
 を備えることを特徴とする請求項 13 記載の否認防止情報管理装置。

【請求項 15】 アプリケーションプログラムにより動作するアプリケーション手段と通信路との間に設けられる否認防止情報管理装置であって、
 上記アプリケーション手段から受け取ったアプリケーションデータに対し電子署名を行う署名部と、
 上記署名付アプリケーションデータを送信先の鍵情報にもとづき暗号化する暗号部と、
 上記暗号化されたアプリケーションデータが蓄積されるログ蓄積部と、
 上記蓄積された暗号化されたアプリケーションデータを通信路へ送信する手段とを具備する否認防止情報管理装置。

【請求項 16】 上記アプリケーション手段からのアプリケーションデータが安全化条件を満たすか否か判定する判定手段と、その判定手段が条件を満たすと判定すると上記アプリケーションデータを上記署名部へ送り、条件を満たさないと判定すると上記アプリケーションデータを上記送信手段へ送る手段とを備えることを特徴とする請求項 14 又は 15 記載の否認防止情報管理装置。

【請求項 17】 クライアント端末からの要求に応じてコンテンツをクライアント端末へ送信するサーバに設けられる否認防止情報管理装置において、
 上記クライアント端末から受信したアプリケーションデータ中の鍵情報が一時保存される保存部と、
 アプリケーションデータに対し電子署名を行う署名部と、
 上記署名付アプリケーションデータを上記保存部の鍵情報にもとづき暗号化する暗号部と、
 上記暗号化されたアプリケーションデータが蓄積される

ログ蓄積部と、
 上記ログ蓄積部に蓄積された暗号化されたアプリケーションデータを上記クライアント端末へ送信する手段とを具備する否認防止情報管理装置。

【請求項 18】 上記クライアント端末から受信したアプリケーションデータは暗号化されたものであり、
 その受信暗号化アプリケーションデータが蓄積されるログ蓄積部と、
 上記受信暗号化アプリケーションデータを復号する復号部と、

上記復号されたアプリケーションデータの署名を検証する検証部とを具備することを特徴とする請求項 14 記載の否認防止情報管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明はクライアント端末における WWW ブラウザと WWW サーバとの通信や電子メールなどにおいて、通信内容を、後で否認するおそれがある情報を、否認できないように管理する方法、その装置及びプログラム記録媒体に関する。

【0002】

【従来の技術】 例えば図 13 に示すようにインターネットを介して、クライアント端末上の WWW ブラウザにより HTML で記述されたテキストを解釈して表示し、希望するファイルやサービスなどを URL（資源指定する手法）により指定して、HTTP プロトコルにより WWW サーバと通信して、WWW サーバより所望の例えばコンテンツを取得することが行われている。この場合、誰が何を注文したかのプライバシーの保護や送信中のコンテンツが盗まれてもそのコンテンツを利用できないようにする点などから、SSL（Secured Sockets Layer）と云われる暗号ソフトウェアで暗号化して通信することが行われている。

【0003】

【発明が解決しようとする課題】 例えばクライアントが注文したコンテンツと異なるコンテンツが送られて来たとサーバに不平を云うようなことがある。この場合、クライアント端末側で注文に関するデータやサーバ側で送信コンテンツに関するデータをログとして記録保存していても、これらは容易に改ざんすることができるため相手を納得させることができない。つまり、そのようなデータを見せても、そのデータは否認されても仕方ないものである。

【0004】 SSL による暗号化は、通信路上でのみ暗号化するものであり、送信先が決れば、送信情報を順次暗号化して、送信し受信側でも、受信信号を直ちに復号して始めてアプリケーションプログラムで解釈することができるものである。従って、従来の SSL により暗号化された通信路上のデータをログとして保存していても、どのクライアント端末又はどのサーバよりのどの通

信データであるかを区別することができない。従って、この通信路上の暗号化通信データを単にログとして保存しておいても、否認防止情報として管理することができず、つまり否認防止情報として用いることはできない。

【0005】

【課題を解決するための手段】この発明によれば、アプリケーションデータ、つまりアプリケーションプログラムが認識できる一塊りのデータごとに署名を付け、必要に応じ暗号化して送信すると共にその署名付アプリケーションデータをログ蓄積部に蓄積しておく。また受信の際に署名付アプリケーションデータをまずログ蓄積部に蓄積し、その後、暗号化アプリケーションデータの場合は復号した後署名検証する。つまりログ蓄積部には一塊りのアプリケーションデータごとに署名が付けられており、アプリケーションプログラムで発信者（端末又はサーバ）、受信者（端末又はサーバ）の区別ができ、必要に応じて日時を付けておけば、後に問題になった時に、対応するアプリケーションデータを取り出して署名を検証することにより、そのデータについて否認できないようにすることができる。

【0006】

【発明の実施の形態】この発明をクライアント端末上のWWWブラウザとWWWサーバとの間における通信に適用した実施例を先ず説明する。図1はクライアント端末11がそのWWWブラウザ12により、WWWサーバ13からインターネットなどの通信網14を介してコンテンツを取得する場合である。ブラウザ12と通信網14の通信路との間にこの発明による否認防止情報管理装置15が設けられる。

【0007】利用者はブラウザ上の画面を見て希望するコンテンツのURLをキーボードにより入力し、又は画面上でマウカを指示させてクリックすると、ブラウザ12からアプリケーションデータとしてリクエスト（Request）データ16が否認防止情報管理装置15に入力される。このリクエストデータ16は例えば図2Aに示すように、コンテンツ取得を示すGET、通信プロトコルhttp、着信アドレス、プログラムのファイル名そのプログラムに対する命令、この例ではファイル名moss.cgi中のコンテンツhtmを安全な状態で取得することを示しており、更に通信プロトコルとそのバージョン番号、プロキシ（代理サーバ）の使用可能、サーバのソフト名などが記述されている。

【0008】否認防止情報管理装置15では図3に示すように、ブラウザ12よりのリクエストデータ16は安全化判定部31に入力されて、コンテンツを安全に、つまり改ざんされたり、盗まれたりしない状態で取得することを要求するか否かの判断が行われる。この例ではセキュア状態で取得する安全化URLリスト17を設け、リクエストデータ16中の取得ファイル名がそのリスト17中にあれば、セキュア用リクエストとする。

【0009】安全化URLリスト17は例えば図2Bに示すように、安全化されるべき各URLが、URLとクライアント名とCA名と鍵番号とを順次「,」で区切られて1行としてそれぞれ記憶されている。CA名はそのクライアント名のクライアントがそのコンテンツ取得のために用いる秘密鍵に対する公開鍵を登録している認証局名であり、鍵番号（Keyse1）はその複数の登録公開鍵の1つを特定するための番号である。図2B中のURLの2行目において「*」印はその前の情報はどのようなものでもよいことを示す。

【0010】図2Aに示した例のリクエストデータ16中のファイル名は「moss.cgi」であり、安全化URLリスト17中の2番目に該当する。よって安全化判定部31は安全化要求をすると判定し、更に取得か否か判断部32ではリクエストデータ16が「GET」であり取得と判断し、鍵情報付加部33でリクエストデータ16に、安全化URLリスト17の該当するURLの格納部から得た鍵情報を付加して図2Cに示すようなセキュア用リクエストデータ18とする。図2C中の破線より下の部分が付加された鍵情報18aであり、一行目が認証局CAに登録されているクライアントのEメールアドレスであり、2行目が認証局CAの識別情報であり、3番目が使用する鍵番号である。このセキュア用リクエストデータ18が通信路へ送信部34を通じて送信される。この通信プロトコルはこの例ではHTTPである。

【0011】サーバ13はHTTPで受信する受信部51（図4）で受信され、否認防止情報管理装置21へ供給され、その受信電文がセキュア用か否かの判定が判定部52で行われる。この判定はその電文のヘッダに付けられている後のデータの種別を表わすMIME Content Typeから行う。セキュア用電文であれば、安全化情報分離部53において、GETであれば、前記例ではセキュア用リクエストデータ18はGETであるからその鍵情報18aが保存部54に保存され、残りのデータはアプリケーション手段55に供給される。

【0012】アプリケーション手段55は、サーバ13のWWWブラウザに対する主要なアプリケーションプログラムを機能させるものである。つまりこの例では、受信したリクエストデータ18中の「moss.cgi?url=/secure.htm」にもとづきコンテンツデータベース22からhtmのコンテンツを取り出し、アプリケーションデータとされたコンテンツが否認防止情報管理装置21に供給される。

【0013】否認防止情報管理装置21では図4に示すように、そのアプリケーションデータとされたコンテンツは安定化されるべきであるかの判定が判定化部56で行われる。この例ではセキュア用リクエストデータ18中の「secure.htm」の「moss.cgi」により安全化することが要求されている。従ってコンテ

7

ントは署名部 57 で鍵記憶部 58 中のサーバ署名用鍵により電子署名が付けられ、この署名付コンテンツは暗号部 59 で保存部 54 に保存された鍵情報にもとづき暗号化される。つまり鍵取得部 61 が鍵管理アプリケーションプログラム 23 を、保存部 54 の鍵情報 18a について実行して、その CAID 情報の認証局装置 24 をアクセスして、鍵情報 18a 中のクライアント E メールアドレスと鍵番号を送り、認証局装置 71 からそのクライアントのその鍵番号の公開鍵証明書を取得する。

【0014】その取得した公開鍵証明書中の公開鍵により暗号部 59 で署名付コンテンツを暗号化する。この暗号化コンテンツ（暗号化アプリケーションデータ）をログ蓄積部 24 に必要に応じてその日時と共に蓄積すると共にその暗号化コンテンツは送信部 62 より HTTP プロトコルにより通信路へ送信される。このセキュア化コンテンツ 25 は例えば暗号化データの国際規格フォーマットである MOSS にフォーマット化されており、そのヘッダに、後のデータの種別を表わす MIME Content Type に暗号化されている記述をする。なおクライアント端末 11 で署名の検証ができるように、署名部 57 の署名に用いた署名鍵と対応する検証用公開鍵を登録してある認証局識別情報 CAID と、その認証局に登録してあるサーバ 13 のアドレスと、署名に用いた鍵の番号 (Key sel) とよりなる鍵情報も、セキュア化コンテンツ 26 にその MOSS フォーマットに従った箇所に記述しておく。

【0015】クライアント端末 11 ではサーバ 13 から送信されたセキュア化コンテンツ 26 は否認防止情報管理装置 15 の受信部 35（図 3）で受信され、安全化情報分離部 36 でそのヘッダの MIME Content Type から暗号化データであると判定して受信セキュア化コンテンツ 26 をログ蓄積部 19 に必要に応じて日時と共に蓄積すると共に復号部 37 で、先にセキュア用リクエストデータ 18 で送った鍵情報 18a と対応する秘密鍵を鍵記憶部 38 から取出して復号する。その復号されたコンテンツを検証部 39 で署名の検証を行う。この検証用鍵は、受信したセキュア化コンテンツ 26 中の鍵情報を用いて、鍵取得部 41 が鍵管理アプリケーションプログラムを実行して登録認証局から登録サーバアドレスの鍵番号の公開鍵証明書を取得して得る。

【0016】その検証に合格すると復号されたコンテンツは HTML 記述状態でブラウザ 12 へ供給され、例えば画面表示される。次にブラウザ 12 からのリクエストが POST の場合でセキュア化リクエストデータとしてサーバ 13 へ送信する例を図 5 を参照して説明する。この場合ブラウザ 12 には図 6A に示すフォームデータ 72 がサーバ 13 から与えられており、そのうちのデータ 72a はサーバ 13 の認証局 CA に登録したアドレス、登録した認証局の識別情報 CAID、使用する鍵番号 (Key sel) よりなる鍵情報であり、これは画面に

8

表示されない。データ 72b は入力された名前を表示する箇所、実行ボタン、リセットボタンが画面に表示されている。名前、図示例では「h o g e h o g e l」を入力して実行ボタンを操作すると、例えば図 6B に示すリクエストデータ 73 がブラウザ 12 から否認防止情報管理装置 15 へ供給される。リクエストデータ 73 は図 2A に示したリクエストデータ 16 に対し、GET が POST に変更され、フォームデータとして付加され、つまり図 6A 中のサーバの鍵情報と、入力された名前などが加わった点以外はほぼ同様である。

【0017】この POST リクエストデータ 73 も図 3 の否認防止情報管理装置 15 内の安全化判定部 31 で安全化条件部 17 の安全化 URL リスト内の URL と一致するか否かにより安全化処理を行うかの判定がなされ、この例では「m o s s . c g i」により安全化処理が行われる。POST リクエストデータ 73 は署名部 42 において、鍵記憶部 38 内のクライアントの署名鍵により電子署名が付けられ、その署名付 POST リクエストデータは暗号部 43 で、そのデータ 73 内のサーバ 13 の鍵情報にもとづき暗号化される。詳しくは先に述べた場合と同様にその鍵情報に基づき、鍵取得部 41 によりサーバ 13 の公開鍵証明書を認証局 71 から取得してその公開鍵により暗号化する。このようにして得られた暗号部 43 よりのセキュア化リクエストデータ 74 は送信部 34 により通信路へ送信される。このデータ 74 の内容は例えば図 6C に示すようなものである。

【0018】このセキュア化リクエストデータ 74 はサーバ 13 の否認防止情報管理装置 21 内の HTTP 受信プログラム処理部、つまり図 4 の受信部 51 に受信され、そのセキュア用電文判定部 52 でセキュア用電文と判定され、更に安全化情報分離部 53 で暗号化された POST リクエストデータと判断されて、ログ蓄積部 24 に日時データと共に蓄積される。またこのセキュア化リクエストデータ 74 は復号部 63 で鍵記憶部 58 内のブラウザ 12 へ送ったサーバ鍵情報と対応する秘密鍵で復号し、その復号された POST リクエストデータの署名の検証を検証部 64 で行う。なおこの検証が可能のように、セキュア化リクエストデータ 74 内の MOSS 化フォームデータ内に、クライアント端末 11 内の署名部 42 の署名に用いた鍵と対応する公開鍵を得るための鍵情報が記述されており、この鍵情報を用いて、認証局から対応する公開鍵証明書を取得し、その公開鍵を用いて検証を行う。

【0019】この検証に合格すると、その復号された POST リクエストデータをアプリケーション手段 55、つまり WWW サーバのプログラムの対応する処理部分により処理させる。このリクエストデータが例えば単なる名前の登録の場合は、その登録を行うと共にその受信したことを示すメッセージを、暗号化することなく送信部 62 を通じてクライアント端末 11 へ送信する。あるいは

は見積書にPOSTリクエストデータ中の名前を記入して、クライアント端末11に返送する。この際に、この内容の見積書を送ったことをクライアント端末11のクライアントが否認できないようにするには、先のコンテンツのクライアント端末11への送信と同様に電子署名を付け、更に暗号化し、その暗号化した回答書をログ蓄積部24に蓄積すると共にクライアント端末11へ送信する。

【0020】上述において、コンテンツデータベース22に格納されているコンテンツに対し、署名部57によりサーバ13の電子署名を付けておき、その署名付コンテンツをデータベース22に格納しておいてもよい。この場合は、コンテンツをクライアント端末11へ送信する。更に署名部57による署名処理が省略でき、それだけ全体としての処理を高速化することができる。クライアント端末11、サーバ13の何れにおいても送信電文を蓄積するログ蓄積部と、受信電文を蓄積するログ蓄積部とを分離して設けてもよい。

【0021】以上述べたように、コンテンツなどの一塊りのアプリケーションデータごとに署名を付けて、暗号化してログ蓄積部に蓄積することができる。よって、必要に応じて所望のアプリケーションデータをログ蓄積部から取出して署名検証により、その情報を署名者が否認することを不可能にすることができる。またこの実施例のように暗号化する場合は、その鍵情報からどこへ送信したかの否認も不可能とすることができる。なお例えば利用者からのログ蓄積部に蓄積したログを確認したい要求があれば、そのログをMIME Content Typeの次のアドレスと、ログ蓄積を行った日付から、ログ蓄積部を検索して、そのログを表示画面に表示する。これによりそのアドレスと日付から、そのログ（アプリケーションデータ）をその利用者がそのアドレスに送ったか否か、又はその利用者が受け取ったか否かを検証し、更に必要に応じてそのログ（アプリケーションデータ）を復号部に復号させ、その復号結果に対する署名を検証部に行わせ、その検証結果の表示を見て、例えば不合格ならそのログは誤りがあるものとして削除したり、合格を確認して利用者が満足すれば、そのログの確認処理を終了する。更に必要に応じてそのログのアプリケーションデータの内容も確認したい要求があれば、先に復号したログを呼び出して表示画面に表示する。なお管理者は古くなり不要となったログの削除なども行う。

【0022】クライアント端末11は例えばパーソナルコンピュータにより構成され、その場合、例えば図7に示すように、安全化URLリストメモリ17、ログ蓄積部19、鍵記憶部33、送信部34、受信部35、ブラウザプログラムが記憶されたメモリ81、否認防止情報管理プログラムが記憶されたメモリ82、鍵管理プログラムが記憶されたメモリ83、コンピュータの基本動作を行う基本プログラムが記憶されたメモリ84、CPU

85がバス86に接続されて、全体としての機能が行われる。なおメモリ81、82、83に対しては対応するプログラムが、外部から予めインストールされるが、対応したプログラムが格納されたものを直接接続してもよい。更に否認防止情報管理プログラムの実行において、署名処理、暗号化処理、復号化処理、検証処理などソフトウェアで行うことなく、モジュール化された復号部37、検証部39、署名部42、暗号部43を利用するようにしてもよい。これらモジュール化したものの利用はその全てに限らず、そのうちのいくつかを行ってもよい。図に示さないがサーバ13も同様にコンピュータを用いた構成とすることができる。

【0023】クライアント端末11側の否認防止情報管理装置15の動作処理の手順は図8に示すようになる。ブラウザ12からリクエストを受信すると（S1）、そのリクエストが安全化（セキュア）条件に該当するかを調べ（S2）、該当しない場合はそのままサーバ13へ送信し（S3）、該当する場合はそのリクエストがPOSTかGETかの判定を行い（S4）、GETの場合は、そのリクエストのHTTP通信プロトコルのヘッダにクライアントの鍵情報を追加し（S5）、サーバへ送信する（S6）。

【0024】リクエストがPOSTの場合は、ブラウザから受信した電文にクライアントの電子署名を付け（S7）、サーバより得たフォームデータ内のサーバ鍵情報を参照し（S8）、その鍵情報をもとに認証局からサーバ公開鍵証明書を取得し（S9）、その公開鍵を用いて前記署名付電文を暗号化し（S10）、その暗号電文をログ蓄積部に保存し（S11）、その後その暗号電文をサーバへ送信する（S12）。

【0025】サーバ13側の否認防止情報管理装置21の動作処理手順は図9に示すようになる。まず受信電文がセキュリティ用か否かを調べ（S1）、セキュリティ用であればその電文、つまりブラウザからのリクエストがPOSTかGETの何れであるかを調べ（S2）、GETであれば、その電文のHTTPヘッダからクライアント鍵情報を取得保存し（S3）、その電文に対応したコンテンツ又は署名付コンテンツをデータベースから取得し（S4）、その取得したコンテンツが署名付でなければ（S5）、そのコンテンツに電子署名を付ける（S6）。また前記保存したクライアント鍵情報にもとづきクライアントの公開鍵証明書を認証局から取得し（S7）、その公開鍵を用いて署名付コンテンツを暗号化し（S8）、その暗号化コンテンツをログ蓄積部に蓄積し（S9）、その後、その暗号化コンテンツをクライアント端末へ送信する（S10）。

【0026】受信電文がPOSTであれば、その電文をログ蓄積部に蓄積し（S11）、その受信電文を復号化し（S12）、また電文中のクライアント鍵情報に基づき認証局からクライアント公開鍵証明書を取得し（S1

3)、その公開鍵を用いて復号された電文の署名を検証し(S14)、その電文がコンテンツの取得要求であればコンテンツデータベースをアクセスし(S15)、ステップS4へ移る。次にこの発明を電子メールに適用した例を図10を参照して説明する。メール端末91とそのメール端末91が所属するメールサーバ92との間に否認防止情報管理装置93が介在され、またメール端末94とその端末94が所属するメールサーバ95との間に否認防止情報管理装置96が介在される。メール端末91と否認防止情報管理装置93間、またメール端末94と否認防止情報管理装置95間はそれぞれメール送信プロトコルSMTPと受信プロトコルPOPで通信が行われ、またメールサーバ92と否認防止情報管理装置93間、またメールサーバ95と否認防止情報管理装置96間もそれぞれ送信プロトコルSMTPと受信プロトコルPOPで通信が行われる。メールサーバ92と95の間も通信が行われる。

【0027】例えばメール端末91から電子メールをメール端末94へ送信する場合に、メール端末91よりのメールは否認防止情報管理装置93に入力される。否認防止情報管理装置93は図3に示した構成とほぼ同様な構成を備え、安全化判定部31で安全化条件に該当するかを調べる。例えば通常のアドレスが図11Aに示す場合にそのアドレス中の「@」を図11Bに示すように「%」に変更し、かつ最後にキーワード「@security」を追加する。この変更はアプリケーションプログラム上で行ってもよいし、メール端末91内のアドレス帳中の、安全にしたいと思われる相手のアドレスをそのように記述しておく。この場合は、安全化判定部31で着信アドレス中にキーワード「@security」があれば安全化、なければ通常の通信と判定する。安全化の場合は図3中に破線で示す指示により署名部42で電子署名を付け、その鍵情報(受信側で検証に必要とする公開鍵を得るための情報、つまりCAID、登録アドレス、鍵番号など)を付加し、また受信者の公開鍵証明書を鍵管理アプリケーションプログラムにより認証局装置71から取得し、その公開鍵により暗号部43で暗号化してMOSSのフォーマットでメールサーバ92へ送る。この際受信アドレスは図11Aに示すような通常のアドレスに戻しておく。またメールサーバ92へ送信すると共にその暗号化メールをログ蓄積部97に蓄積する。

【0028】メールサーバ92はその暗号化メールをメールサーバ95へ送り、メールサーバ95はその暗号化メールを否認防止情報管理装置96へ供給する。否認防止情報管理装置96も図3に示したものとほぼ同様な構成であり、安全化情報分離部36でそのMOSSフォーマットのヘッダのMIME Content Typeから安全化されたものと判断されるとログ蓄積部98

(図10)に蓄積すると共に復号部37で復号し、その

復号されたメールの署名を検証部39で検証し、検証に合格するとそのメールをメール端末94へ送る。検証部39における送信者の検証用公開鍵の取得は先に述べたと同様な手法による。安全化情報分離部36で暗号化されたものでないと判断されるとそのままメール端末74へ送信される。

【0029】図11Cに示すように、安全化アドレスのキーワード「@security」の後に、楕円DH暗号の相手が使用する秘密鍵番号に対する公開鍵番号と、自分が使用する秘密鍵番号と、自分が署名に用いる鍵番号とを記述しておいてもよい。この例ではこの相手の公開鍵番号の鍵と、自分の秘密鍵とにより共通鍵を生成してアプリケーションデータを暗号化する例である。図12に示すように安全化して送信したい相手のアドレスとその相手の秘密鍵と対応する公開鍵が登録されている認証局アドレスと、その認証局に登録してある相手のアドレスと、使用する暗号形式と、使用する鍵番号とを組とするリストを作っておき、図3中の安全化条件部17に格納しておき、送信メール端末から受信したメールのアドレスが安全化条件部17にあるか否かを安全化判定部31で判定し、あればその安全化条件部17のリスト中の該当するアドレスについて格納されている鍵情報を用いて受信者の公開鍵を取得して、暗号部43で暗号化するようにしてもよい。

【0030】なお図11に示した例でアドレス帳を用いる場合は、同一受信者についても、通常アドレスと安全化アドレスとの両者をアドレス帳に記入しておき、その何れかを選択使用できるようにすることもできる。図10から容易に理解されるように1つのメールサーバ92に所属する複数のメール端末を1つの否認防止情報管理装置93により一元的に否認防止情報を管理することもできる。また複数のプロトコルを利用する複数のアプリケーションの一元的に否認防止情報を管理することができる。要はこの発明によれば、後で否認されるおそれのある情報については、その一塊りのアプリケーションデータを署名し、必要に応じて暗号化した状態で、送信情報も、受信情報もログ蓄積部に蓄積しておけばよく、そのアプリケーションデータを作るアプリケーションプログラムには任意のものでよく、否認防止情報管理装置で送信の際はそのアプリケーションデータが否認されるおそれがあるものであるか否かの判断ができるようにすると共に、受信の際はそれが安全化アプリケーションデータとされたものであるか否かをMOSSのヘッダのMIME Content Typeなどで区別できればよい。上述では暗号化を公開鍵暗号方式により行ったが、例えばコンテンツを共通鍵で暗号化し、その共通鍵を公開鍵暗号方式により暗号化して同時に送り、受信側で共通鍵を復号し、復号した共通鍵でコンテンツを復号するようにしてもよい。

【0031】暗号化する場合は、アプリケーションデー

タの全体を暗号化し、その暗号化データにヘッダとして MIME Content Type と、相手先アドレスを更に付ける。上述の説明から明らかなように否認防止のアプリケーションデータにて必ず署名を付けるが、暗号化はしなくてもよい。

【0032】

【発明の効果】以上述べたように、この発明によればアプリケーションレベルで一塊りのアプリケーションデータに対し署名を付けてあり、これをこの単位で区別して送信時にも、受信時にもログ蓄積部に蓄積でき、しかもそのデータを思うように改ざんすることはできないため、後でそのようなデータを送ってないとか、受信していないとか、問題が生じた場合にそのログ蓄積部に蓄積されている該当するものを署名検証することにより、当初のデータの正当性を否認することができないことになる。また前記例のように暗号化する場合はその復号のための鍵情報からどこへ送信したかも否認することができなくなる。

【図面の簡単な説明】

【図1】 この発明をブラウザとサーバ間の通信に適用した実施例の機能構成を示す図。

【図2】 図1で用いられるGETリクエストデータ16の例を示す図、Bは安全化URLリストの例を示す図、Cはセキュア用リクエストデータ18の例を示す図であ

る。

【図3】 図1中のこの発明による否認防止情報管理装置15の実施例の機能構成を示す図。

【図4】 図1中のこの発明による否認防止情報管理装置21の実施例の機能構成を示す図。

【図5】 この発明をブラウザとサーバ間の通信に適用した他の実施例の機能構成を示す図。

【図6】 Aはサーバより受信したフォームデータ72の例を示す図、Bはリクエストデータ73の例を示す図、Cはセキュア化リクエストデータの例を示す図である。

【図7】 図1中のクライアント端末11をコンピュータにより機能させる場合の機能構成を示す図。

【図8】 図3に示した否認防止情報管理装置15の動作手順の例の一部を示す流れ図。

【図9】 図4に示した否認防止情報管理装置21の動作手順の例の一部を示す流れ図。

【図10】 この発明を電子メールに適用した実施例の機能構成を示す図。

【図11】 Aは通常アドレス、B及びCは安全化アドレスの各例を示す図である。

【図12】 安全化アドレスリストの例を示す図。

【図13】 従来のクライアントとサーバ間の暗号化通信を説明するための図。

【図1】

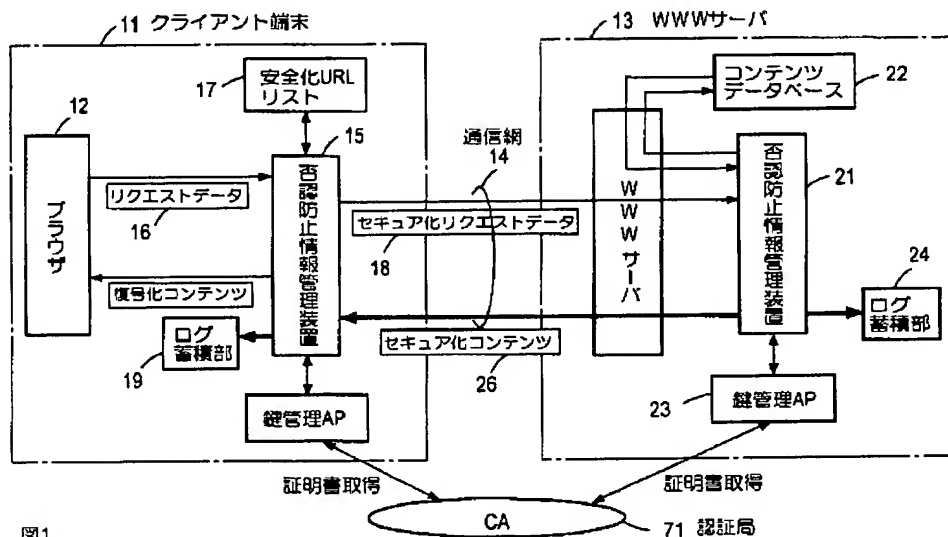
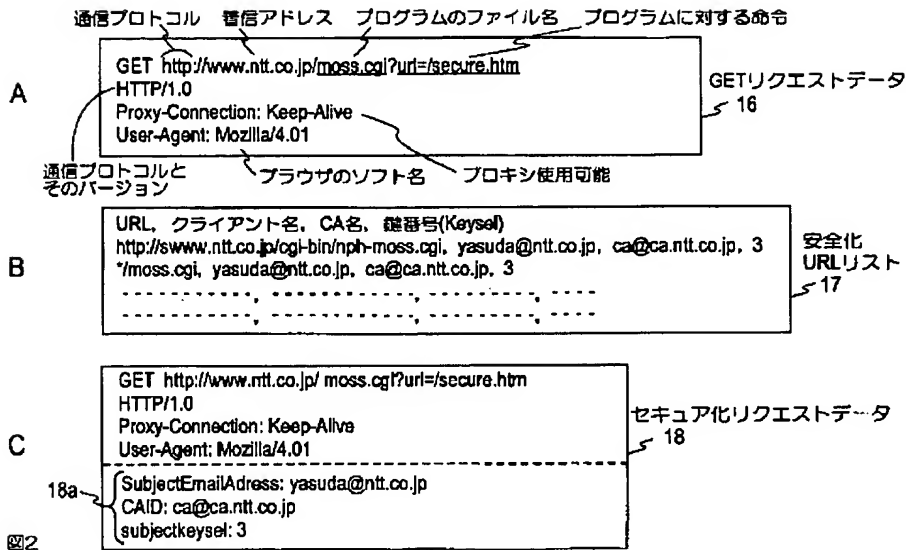
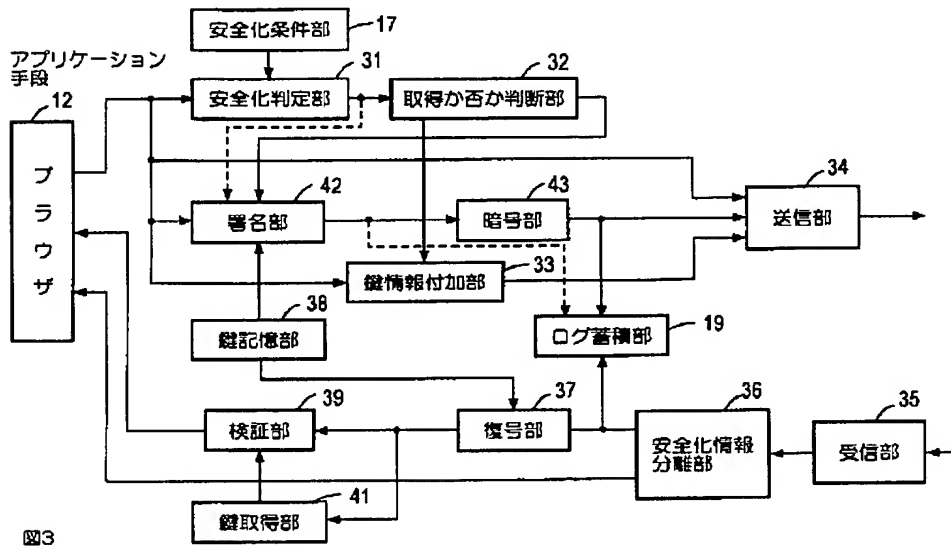


図1

【図 2】



【図 3】



【図 1 1】

通常アドレス yasuda@ntt.co.jp

安全化アドレス yasuda% ntt.co.jp@security

// yasuda% ntt.co.jp@security [相手DHkeyset[自分DHKeyset[自分EsignKeyset]]]

図11

【図 1 2】

アドレス	認証局アドレス	登録アドレス	格号形式	鍵番号
yasuda@winca	ca@winca	yasuda@winca	E-DH256	4
ogihara@winca	ca@winca	ogihara@winca	E-DH256	6
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮

図12

【図 4】

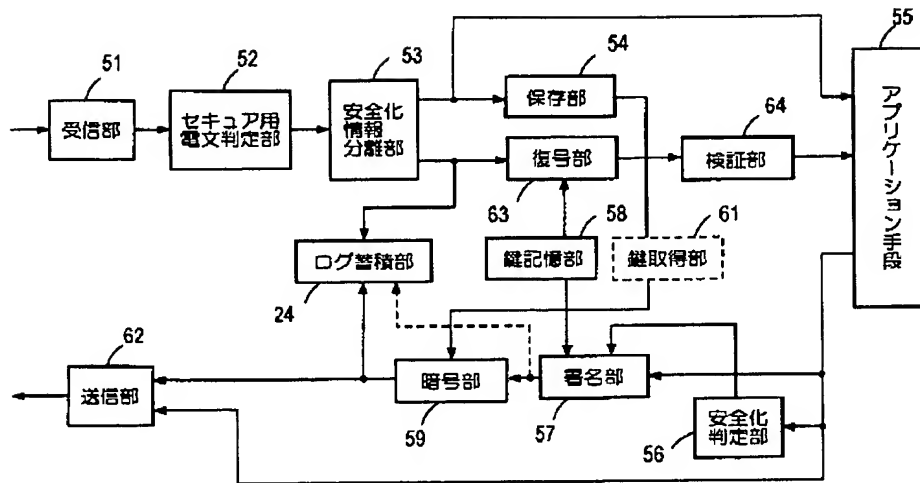


図4

【図 5】

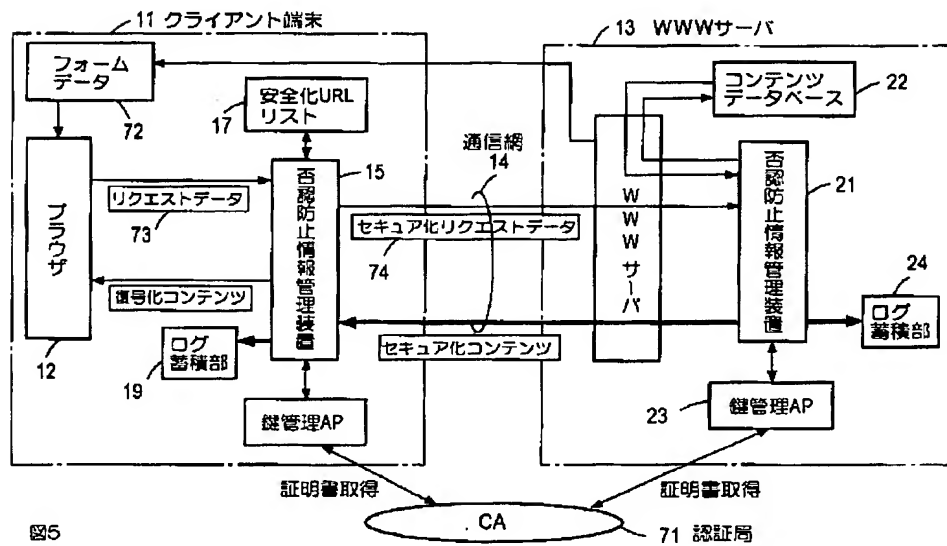


図5

【図 13】

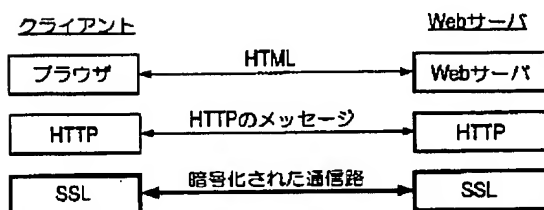


図13

【図 6】

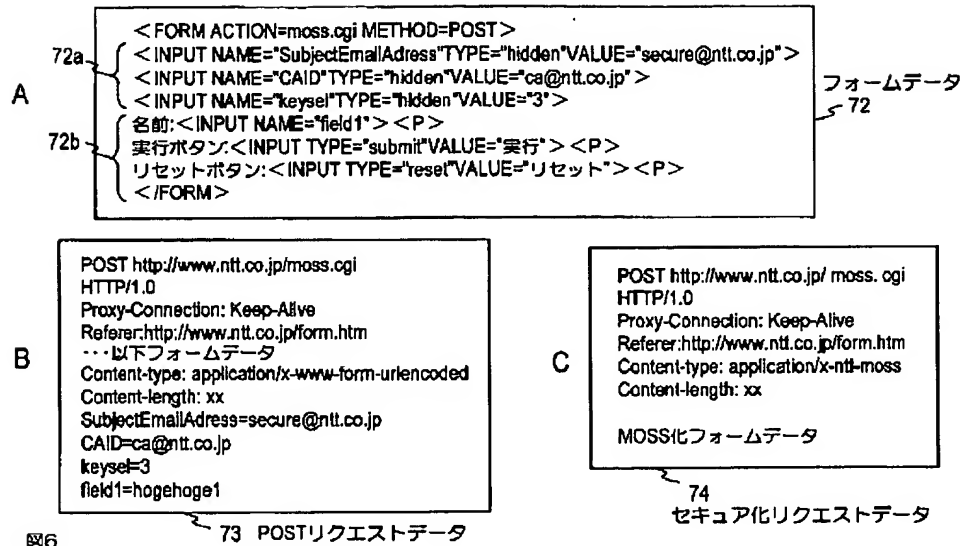


図6

【図 7】

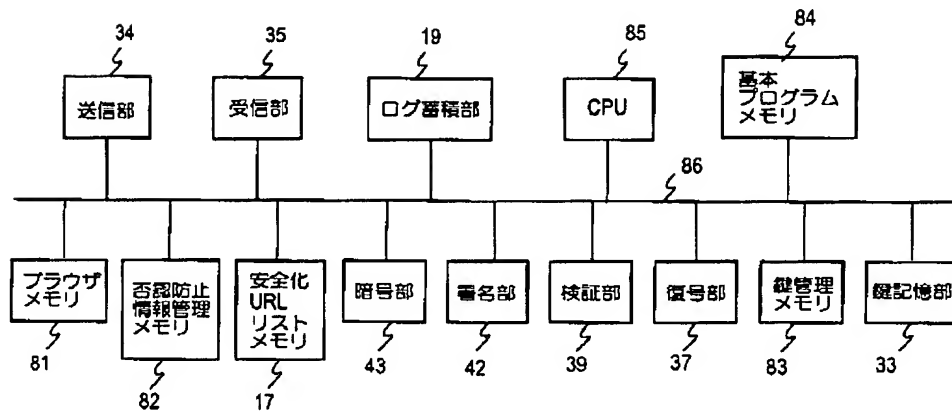


図7

【图 9】

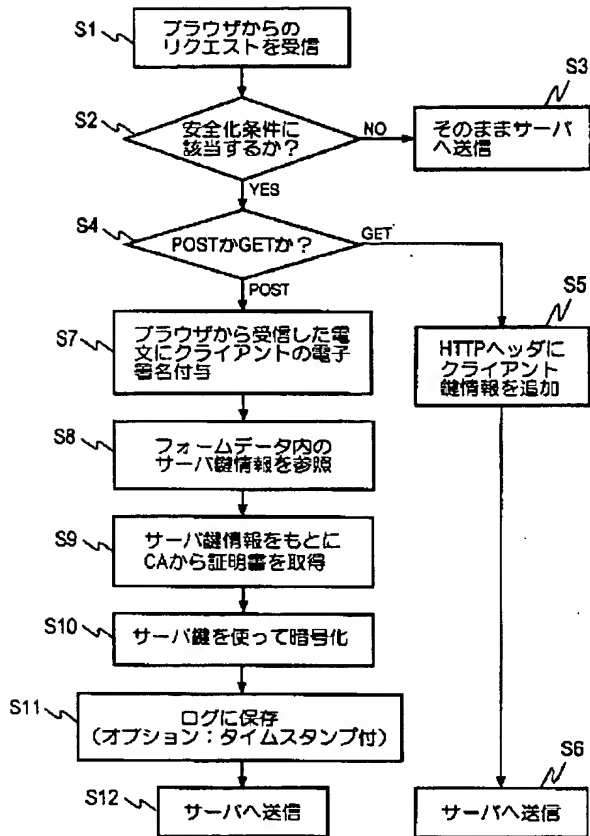


图 8

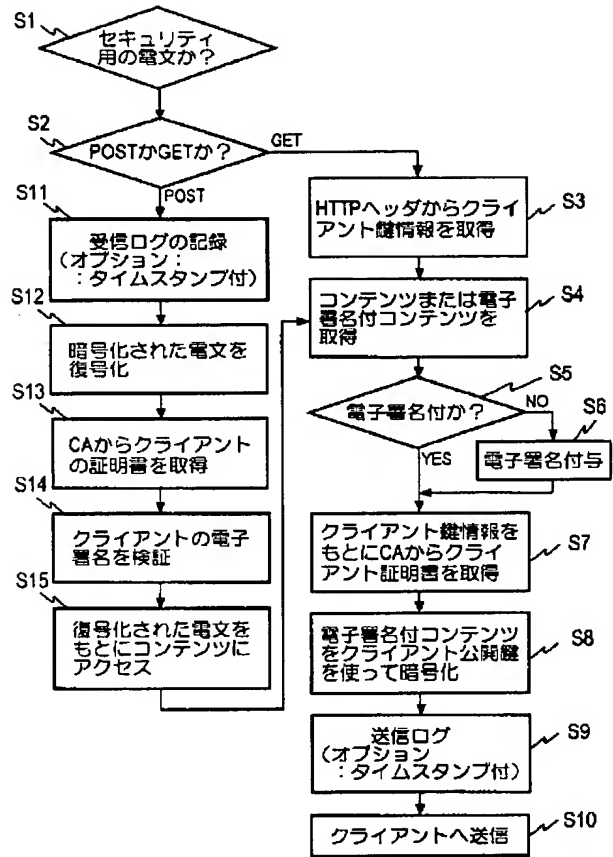


图9

【図 10】

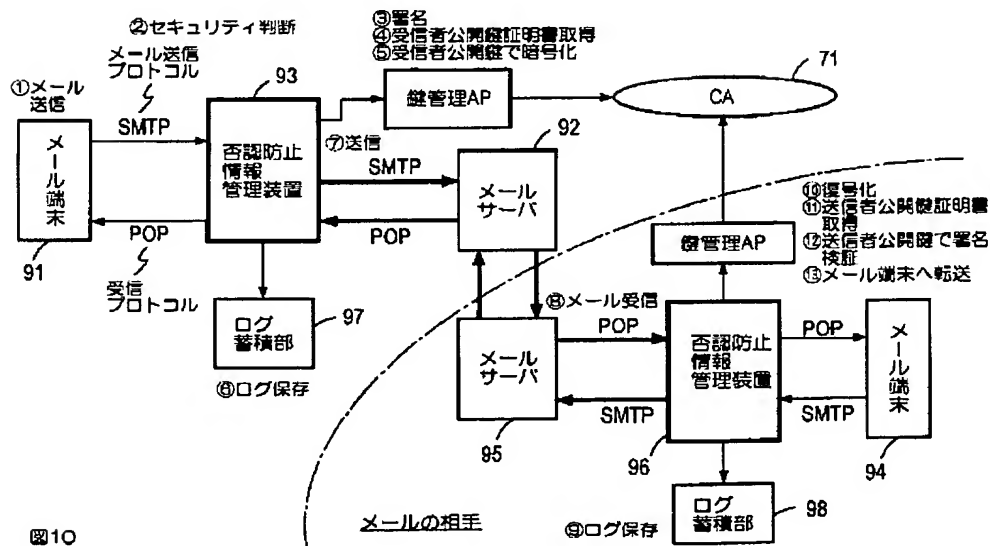


图 10

フロントページの続き

(72)発明者 渡辺 徹
東京都千代田区内幸町一丁目 1 番 6 号 エ
ヌ・ティ・ティ・コミュニケーションズ株
式会社内

(72)発明者 荻原 利彦
東京都千代田区内幸町一丁目 1 番 6 号 エ
ヌ・ティ・ティ・コミュニケーションズ株
式会社内

(72)発明者 田淵 博康
東京都千代田区内幸町一丁目 1 番 6 号 エ
ヌ・ティ・ティ・コミュニケーションズ株
式会社内

F ターム(参考) 5B017 AA08 BA07 CA16
5B085 AC14 AE13 AE29 BG07
5J104 AA09 LA03 LA06 MA02 NA02
PA08 PA09